

UNITED STATES PATENT APPLICATION

of

DAVID L. HECHT

JOHN LENNON

and

RALPH MERKLE

for

A RECORD AND RELATED METHOD FOR STORING
ENCODED INFORMATION USING
OVERT CODE CHARACTERISTICS TO IDENTIFY
COVERT CODE CHARACTERISTICS

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N.W.
WASHINGTON, DC 20005
202-408-4000

BACKGROUND OF THE INVENTION

This invention relates to self-clocking glyph codes for recording digital information on graphic recording media, such as plain paper. Even more specifically, this invention pertains to techniques for increasing the security of the digital information while preserving the homogenous visible appearance of the resultant product.

Distinguishing copies or counterfeits of original authentic documents is a common important objective. Printing documents with features that are difficult to copy or counterfeit is one general approach to counterfeit suppression. Excellent advanced image copying technology, however, makes it more difficult to print image characteristics that are adequately copy-proof. Special physical printing, such as holograms, can be employed. However, this approach requires special printing equipment and may be counterfeited if that equipment is accessible to the counterfeiter.

Covert chemical taggants are known and have been incorporated into print material such as paper and/or toner. However, counterfeits could be made if the materials making up the chemical taggants could be obtained and applied in the required pattern. Such copying is facilitated if the taggants occur in a distinguishable manner, that is, if the taggants are visually detectable or capable of being detected by optical machine, such as is the case when using tagged yellow toner as a taggant.

Robust self-clocking glyph codes are known. Such codes can generally encode arbitrary digital message codes up to a certain capacity, typically several hundred bytes per square inch. Glyph codes typically comprise distinguishable rotated marks; for example, 3,600 such marks per square inch may form a rectangular lattice. These glyph codes can include encrypted messages, including digital signatures such as

those used in secure electronic communications. However, conventionally printed glyph codes are readily copyable, thereby reproducing their information content. Simply printing glyph codes with a taggant material can be counterfeited if the taggant material can be obtained.

Accordingly, an object of the present invention is to provide a record and related method for encoding information which cannot easily be copied or otherwise counterfeited.

SUMMARY OF THE INVENTION

*Sub
a1* → ~~In accordance with the present invention, a record for storing encoded-~~
information is provided comprising a storage medium, such as plain paper; first marks on the storage medium having a covert code characteristic, these first marks conveying a first message, which may be encrypted; and second marks on the storage medium, which second marks convey an overtly marked code useful in detecting and decoding the first message. In one embodiment, the second marks have an overt code characteristic, whereas the covert code characteristic of the first marks is visibly undetectable. Additionally, the covert code characteristic of the first marks does not affect the appearance of the first or second marks. Also, both the first and second marks comprise glyphs, with the first marks having an additional covert code characteristic, such as a chemical taggant.

In another embodiment, the first marks have a covert code characteristic provided by chemical taggants and are divided into first and second sets of marks. Only the second set of marks conveys an authentication code pattern whose checking is aided by the message in the overtly marked encrypted code. By way of example, the

covertly marked code may comprise authentication data and further by way of example, the overtly marked code may identify the location and logical order of the first set of marks conveying the covertly marked code, which may be encrypted.

It should further be understood that the first and second marks may, at least in part, comprise the same marks. For example, a glyph having a visibly undetectable code characteristic, such as would be provided by a chemical taggant, may also have a visible detectable overt code characteristic as could be provided, for example, by the orientation of a glyph. Thus, that same glyph may function to provide part of both the covert and the overtly marked code.

Of course, it should further be understood that the record of the subject invention may very well, and likely does, include third marks that do not participate in the function of the first and second marks, but which do participate in the storage of at least a portion of the encoded information to be carried by the record.

The invention further comprises a related method for storing encoded information on a storage media, generally comprising the steps of: placing the first marks on the storage media, with the first marks conveying a covertly marked code and placing second marks on the storage media adapted to convey an overtly marked code useful in decoding the covertly marked code, wherein the second marks have an overt code characteristic.

BRIEF DESCRIPTION OF THE DRAWINGS

Still further objects and advantages of this invention will become apparent when the following detailed description is read in conjunction with the attached drawings, in which:

Fig. 1 illustrates a self-clocking glyph code pattern, with the glyphs overtly encoded by the rotational position of a slash-mark glyph character for encoding the overtly marked code;

Fig. 2 illustrates by dashed marked glyphs which are marked distinguishably by the covert marking characteristic and convey an overtly marked code useful in decoding the covertly marked code, which may be encrypted, referenced with respect to Fig. 3;

Fig. 3 illustrates by an additional dot a selected set of glyph marks bearing a covert code characteristic, which marks thereby convey an authentication pattern when information about the set and message are provided by the overtly marked code; and

Fig. 4 shows a code similar to that of Fig. 3, with mixed data (0,1) rotation overt coding.

DETAILED DESCRIPTION OF THE ILLUSTRATED EMBODIMENTS

While the invention is described in some detail herein below with reference to certain illustrated embodiments, it is to be understood that there is no intent to limit the invention to those disclosed embodiments. On the contrary, the intent is to cover all modifications, alterations, and equivalents falling within the spirit and scope of the invention as defined by the appended claims.

As noted above, this invention is directed towards applications and related methods for imprinting on documents dual characteristic covert glyph codes that are very difficult to reproduce or counterfeit. One overt characteristic, such as glyph rotation, is used to encode an overtly marked code that specifies a second covert state characteristic of some or all of the glyphs. The covert characteristic is preferably difficult to detect or copy on a glyph-by-glyph basis and preferably has negligible effect

on the appearance of the glyph in the original document. An example of a covert characteristic is the presence of distinguishable chemical taggants of one or both of two marking materials with indistinguishable visual and photocopy characteristics, as could be obtained, for example, from two chemically different black toners.

In one embodiment, self-clocking glyphs are combined with encrypted messages in overtly marked codes to provide robust and secure identification of covertly marked codes. The overtly marked codes may or may not be encrypted. One example of a self-clocking glyph with rotational overt coding is shown in Fig. 1. As may be seen in Fig. 1 for purposes of clarity, a sync code encoded by predefined glyphs is shown in a "0" glyph state, that is, with the slash of a glyph rotated from upper left to lower right, and variable data glyphs are shown Fig. 1 in "1" glyph state, that is, the rotation of the slash is from upper right to lower left. As shown in Fig. 1, therefore, "0" state glyphs 10 thus form vertical sync lines 14 and horizontal sync lines 16 that provide a rectangular border to a plurality of "1" state glyphs 12, as is conventional in the art. A typical glyph code embodiment has mixed patterns of 1's and 0's in both data and sync codes, thus providing a random-like appearance. It should also be understood, as used herein, the "0" and "1" state of a visible glyph is merely one example of an overt code characteristic that may be used in accordance with the present invention. Other visible modifications, such as glyph shape or glyph orientation, may be employed, as should be understood by those skilled in the art. The covert mark may be one of many types, such as a chemically or physically detectable taggant.

In accordance with the present invention, second marks are provided on the media that convey an overtly marked code useful in decoding the covertly marked code.

As shown in Fig. 2, for example, overt glyph markings are shown as having different rotations. The covert marked glyphs are in two states, denoted in Fig. 2 by solid line and dashed line glyphs (e.g., glyph 30). In one possible embodiment, the overt pattern of glyphs provides an identification of the location of covertly coded glyphs, or a subset of covertly coded glyphs that carry the covertly marked code and the authentic contents of that message; that is, the covert marking state of those glyphs.

Sub
A2
→ ~~Various coding methods that are known to those skilled in the art may be~~
employed and, thus, there are many possible coding schemes for encoding the overt and covert codes employed in the subject invention. The overt glyph code can use, for example, any of the existing glyph code approaches including systems incorporated in commercial glyph encoding software, such as Xerox SDK. Generally, for a pattern including N1 glyphs, a smaller number of user message glyphs N2 will be available. The difference between N1 and N2 is required due to overhead functions, such as synchronization, header or key codes, error correction protection, and spatial pattern filling. Typically, N1 may comprise 3600 glyphs per square inch of glyph coded print. ~~Typically, N2 is greater than half of N1.~~

In one embodiment, the overtly marked code may be carried by N3 overt messaging bits, namely N3 clear text or visible messaging bits, N4 encrypted user message bits and N5 bits for desired error protection overhead. Thus, it is required that N2 be greater than or equal to $N3 + N4 + N5$. As was noted above, the overtly marked code carried by the $N3 + N4 + N5$ bits is used to specify the covert marking code pattern. In other words, this overtly marked code is used to specify which glyphs are marked in which covert state, thereby providing information that is useful in decoding

and authenticating the covertly marked code. The covertly marked code may also be encrypted.

The N3 and N4 bits may thus be used to decode the overtly marked code, which in turn may comprise data from a trusted printing management system, individual print number, usage rights, print owner, digital signature, private message, financial transaction records, or the like, as well as information about the covert marked code. The covert marked code may also carry similar types of trusted printing information.

As referenced above, it is not necessary that all N4 bits carry the overtly marked code. It is instead possible that a smaller number, N6 be specified, while the remaining glyphs of N4 may be encoded pseudo randomly or arbitrarily. The same is true with respect to the glyphs having the covert code characteristics. Not all of the glyphs selected to bear covert code characteristics are necessarily required to convey the covertly marked code. It is desirable to force a potential counterfeiter to try to counterfeit the state of every glyph, both with respect to overt and covert code characteristics. Accordingly, it is desirable for every one of the N1 glyphs to be eligible for possible inclusion as bearing the covert and/or overtly marked codes. However, the number of glyphs actually carrying the covertly marked code should be large enough so that 1 in 2^{N6} random successful matches in counterfeiting attempts is acceptable where N6 is the number of glyphs actually carrying the covert marked code.

There are several examples of possible encoding using the N4 encrypted user message bits. The N4 bits may be used to explicitly define the identity (glyph pattern position) and state of the N6 glyphs bearing the covertly marked code. Generally, identification of one among N1 ordered glyphs in the total pattern requires N7 bits,

wherein N_7 bits equals approximately $\log_2 N_1$ bits for address, plus 1 bit for the state of a two state covert encoding. In general, for R state covert marked encoding, N_7 equals $\log_2 N_1 + \log_2 R$. Thus, N_4 is greater than or equal to $N_6 \times [1 + \log_2 N_1] = N_6 \times N_7$

Examples:

$N_1 = 638$, $N_2 = 11$, $N_6 = 16$, $N_4 = 176$ (22 bytes), $N_5 = 168$ (14 bytes), $N_3 = 32$ (4 bytes), $N_2 = 320$

$N_1 = 1024$, $N_7 = 11$, $N_6 = 8$, $N_4 = 88$ (11 bytes), $N_5 = 32$ (40 bytes), $N_3 = 128$ (16 bytes), $N_2 = 536$

$N_1 = 2048$, $N_7 = 12$, $N_6 = 10$, $N_4 = 120$ (15 bytes), $N_5 = 600$ (75 bytes), $N_3 = 256$ (32 bytes), $N_2 = 976$

$N_1 = 4096$, $N_7 = 13$, $N_6 = 24$, $N_4 = 312$ (39 bytes), $N_5 = 1600$ (200 bytes), $N_3 = 256$ (32 bytes), $N_2 = 2168$

$N_1 = 4096$, $N_7 = 13$, $N_6 = 24$, $N_4 = 1112$ (139 bytes), $N_5 = 1600$ (200 bytes), $N_3 = 256$ (32 bytes), $N_2 = 2968$

Alternatively, the N_4 bits may indirectly identify the N_6 glyphs by pointing to a reference or by providing an algorithm, which may use some or all of the quantities N_1 and N_6 as parameters.

The use of the approaches discussed above can be made most effective through appropriate selection and implementation of encryption and authenticity management protocols. Some desirable approaches which appear practical follow. Referring to the coding methods discussed above, the encryption may implement an existing secret key encryption algorithm. The N_3 overt clear text message bits may be used to specify the identity of secret encryption/decryption keys which are held by a secure server. The

decoded message of the overtly encoded glyph code may be provided to the server along with sufficient authorization credentials of the user/entity/client testing the document. The server decrypts the encrypted code using the appropriate decryption key and returns information specifying which glyphs to test for covert encoding. The server may also hold, access and deliver to the client information required for successful testing; for example, taggant identity, chemical test procedure, optical test procedure to the authorized client, preferably using secure specifications specified by bits in the overtly marked code of size $N3 + N4 + N5$.

Security loss of the glyph test pattern will only compromise the specific document at issue. Security loss of the test method may only help an unauthorized party test other documents otherwise known to involve the same test procedure. However, the test glyph pattern of these other documents would not necessarily be compromised.

A similar overall approach may be developed to other coded mark systems than discussed above, provided they have sufficiently robust addressing (mark logical ordering) characteristics. Examples include checkerboard codes and encoded alphanumeric string codes.

In accordance with the present invention, certain of the glyphs on the printed medium are selected to convey a covertly marked code, which may be encrypted. For example, as shown in Fig. 3, glyphs 20a through 20o are selected to carry a covert code pattern. The overtly marked code, such as the overt code shown in Fig. 1, provides information to identify the covert pattern glyphs and how to decode and/or verify them. For example, the information might include their pattern, covert marking state, logical order, or message.

Examples of covert code characteristics include image modulation, metamers, and visible twin materials. Covert image modulation may be obtained by small glyph translations, or small grey-scale modulations of glyphs by mark intensity or size, provided that such modulations and/or translations are sufficiently small to be difficult to detect or reproduce. Metamers may comprise combinations of marking materials with the same color appearance but different detailed spectral characteristics.

The use of a completely visibly indistinguishable material to provide a covert code characteristic is effective. One possible example is the use of materials with different infrared fluorescent or reflective characteristic. Another example is the use of materials with different ultraviolet fluorescent or reflectance characteristics, which may be resolvable only by a specially tailored filter or instrument. Small spectral differences can make such covert code characteristics difficult to be duplicated through counterfeiting.

One embodiment of covert code characteristic utilizes chemical distinction that requires a separate chemical test on each glyph, i.e., the use of taggants. One possible method of incorporating taggants is to make an atomic substitution of one or more of the components of a toner. An example may be to replace the hydrogen atom on a charge control agent "cetyl pyrridinium chloride." Substitution of the chlorine with bromide or iodine will cause a charge control agent change, which will most likely perform similar for all practical or visual purposes but in fact will be chemically different and can be so detected. A second desired characteristic for the authentication process will be met in that the print area containing this type of substituted material will be extremely small and difficult to locate or quantify except with highly specialized

equipment. Electron dispersive x-ray analysis is capable of analyzing areas down to approximately one square micron for elementary compositions as low as 0.5%. The sensitivity of the technique is enhanced if the material is not homogeneously spread throughout the sample, but is located in clumps as is the case with some charge control agents that are surface active agents.

A still further possible example of covert code characteristics is the use of an isotropically enriched material such as chlorine-37 enriched CPC.

A still further example of a covert code characteristic is to incorporate a reactive chemical into the toner that forms the glyphs, which reactive chemical would combine with an applied solution of a second material to form a unique chemical product that would be quantified by a spectroscope or other comparable method.

Each of the above examples provides glyphs that are physically indistinguishable, but which provide additional information through the applied covert characteristic.

It should be understood that glyphs marked with a covert code characteristic should be printed with adequate relative registration so that such glyphs cannot be distinguished on the basis of a systematic spatial shift between the patterns of glyphs containing or not containing the covert characteristic or a pattern of glyphs containing two or more different states of the covert characteristic. Some printing technologies can provide excellent co-registration of printing of two marking materials. Tri-level xerography is one such example. Xero-colography may also enable effective co-registration of more than two covert marking characteristic materials. If the overt and covert characteristics are provided as part of the same marking process, registration

202-408-4000

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N.W.
WASHINGTON, DC 20005
202-408-4000

may be straightforward. Misregistration may, in the alternative, be masked by pseudo-random two-dimensional translational displacement of individual glyphs from a nominal glyph center pattern.

In accordance with one embodiment of the present invention, only a subset of the covertly marked glyphs are used to convey a covert code. For example, such a covert code may include an authenticity code, a digital signature, or a record numbering data, or the like. In one embodiment, less than all of the glyphs tagged with a covert code characteristic are used to convey the covertly marked code. Accordingly, decoding for this embodiment requires not only identification of marks having a covert code characteristic, but also identification of the subset of such marks that actually carry the covertly marked code. This identification is aided by the overtly marked code.

Fig. 4 shows a code similar to that of Fig. 3, with mixed data (0,1) rotation overt coding. Covert code glyphs are denoted by circles, instead of dots as in Fig. 3.

Accordingly, an approach has been disclosed which may be used to deter copying and counterfeiting of original printed documents so that they may be adequately trusted as authentic originals. Additional incorporated digital printed messages (plain text and/or encrypted and/or digital signature) can be authenticated as original printed entities and thereby distinguished from copies, counterfeits or forgeries. This is useful for document management information, including other authentication data such as data from a trusted printing management system, individual print number, usage rights, print owner, digital signature, private message, financial transaction record and the like.



Counterfeiting of dual characteristic covert glyph codes of the kind disclosed herein requires detection of the covert state of all or most of the glyphs in the counterfeit document or document portion, or requires breaking or stealing the digital encryption code, which can generally be made not practical using existing encryption security methods, as well as requiring access to the covert marking material and equipment for marking the covert states.

However, authentication can be accomplished with a test of relatively few specific glyphs, preferably checking for a similar number of glyphs in each covert state. As illustrated by the above example, authentication can be accomplished using less than or equal to N6 glyphs. The degree of difficulty in trying to reproduce or detect the covert state of each glyph can, therefore, be tailored by the selection of suitable covert encoding methodologies. Thus, robustness of foiling counterfeiting can be scaled from preventing casual copying on standard copies to glyph-by-glyph analytical testing.

The subject invention nevertheless provides the advantageous property of aesthetic appearance, which makes its use practical in many situations where as other marked patterns would be unacceptable.

The foregoing description of the invention has been presented for purposes of illustration and description. It is not exhaustive and does not limit the invention to the precise form disclosed. Modifications and variations are possible in light of the above teachings or may be acquired from practicing of the invention.